



(12) United States Patent
Flavin et al.

(10) **Patent No.:** US 6,219,788 B1
(45) **Date of Patent:** Apr. 17, 2001

- (54) WATCHDOG FOR TRUSTED ELECTRONIC CONTENT DISTRIBUTIONS**

5,838,790 * 11/1998 McAuliffe et al. 743/176

OTHER PUBLICATIONS

- (75) Inventors: **Robert Alan Flavin, Yorktown Heights; Perwalz Nihal, Fishkill; Ronald Perez, Mount Kisco; Sean William Smith, Cornwall, all of NY (US)**

The Patent Office of the UK Search Report dated Oct. 27, 1999 for GB 9906344.8.

J. Schick, "AdJuggler", available via the internet at: <http://www.designshops.com/pace/ds/pub/98/04/17/tools/adjug-gler.html>, pp. 1-4, Apr. 17, 1998.

"NetGravity Launches AdServer 3.0", available via the internet at: <http://www.netgravity.com/press/announce30.html>, pp. 1-3, Mar. 11, 1997.

* cited by examiner

Primary Examiner—James P. Trammell

Assistant Examiner—Pierre Eddy Elisca

(74) *Attorney, Agent, or Firm*—Louis P. Herzberg

- (73) Assignee: **International Business Machines Corporation, Armonk, NY (US)**

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: 09/078,671

(22) Filed: May 14, 1998

(51) **Int. Cl.⁷** **G06F 11/30**

(52) U.S. Cl. 713/194; 713/200; 380/202;
380/203; 348/7; 348/10; 705/51; 705/53

(58) **Field of Search** 348/7, 1, 8, 10,
348/152, 385, 143, 150; 395/226, 210;
713/200, 160, 201, 170, 176, 202, 194;
380/255, 202, 239, 203, 281, 204, 283,
284; 705/10, 26, 51, 53, 64, 67, 68, 69,
75, 76, 80; 455/2

(56) **References Cited**

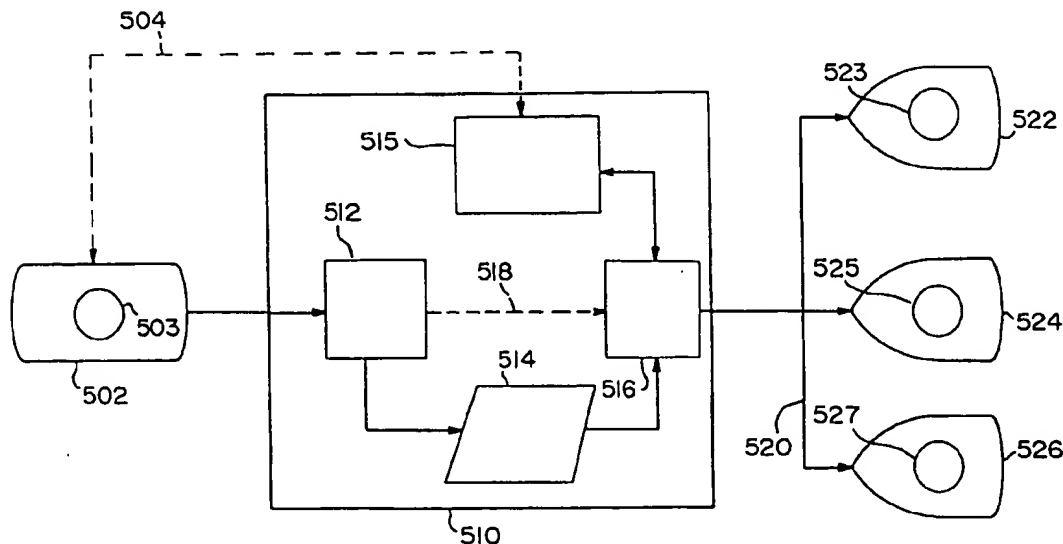
U.S. PATENT DOCUMENTS

4,602,279	*	7/1986	Freeman	358/86
5,144,663	*	9/1992	Kudelski et al.	380/16
5,216,515		6/1993	Steele et al. .	
5,231,494	*	7/1993	Wachob	358/146
5,359,508	*	10/1994	Rossides	364/401
5,515,098	*	5/1996	Carles	348/8
5,724,521	*	3/1998	Dedrick	705/26
5,774,534	*	6/1998	Mayer	379/142

(57) **ABSTRACT**

A computer watchdog system monitors and controls distribution content sent from producers, through distributors, to subscribers. The computer watchdog system acting to ensure the just execution of agreements between a producer of content and a distributor of content. The computer watchdog system serving as an agent trusted by both producers and distributors. The computer watchdog system may be equipped with tamper protection for resisting exogenous attempts to gain unauthorized access to the system. The computer watchdog system may be installed entirely within distributor's sites. Alternatively, the computer watchdog system may reside partially within distributor's sites and partially within subscriber's sites. The computer watchdog system logs and reports on information relating to the distribution of content. Further, the computer watchdog system may selectively transform content provided by a producer, customizing the content for distributors and subscribers.

29 Claims, 6 Drawing Sheets



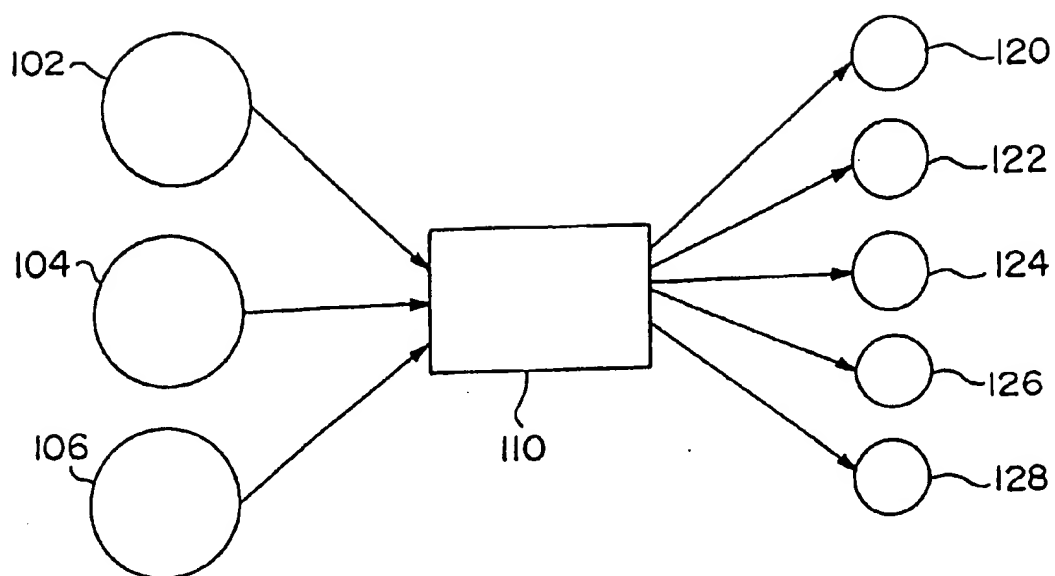


FIG. 1

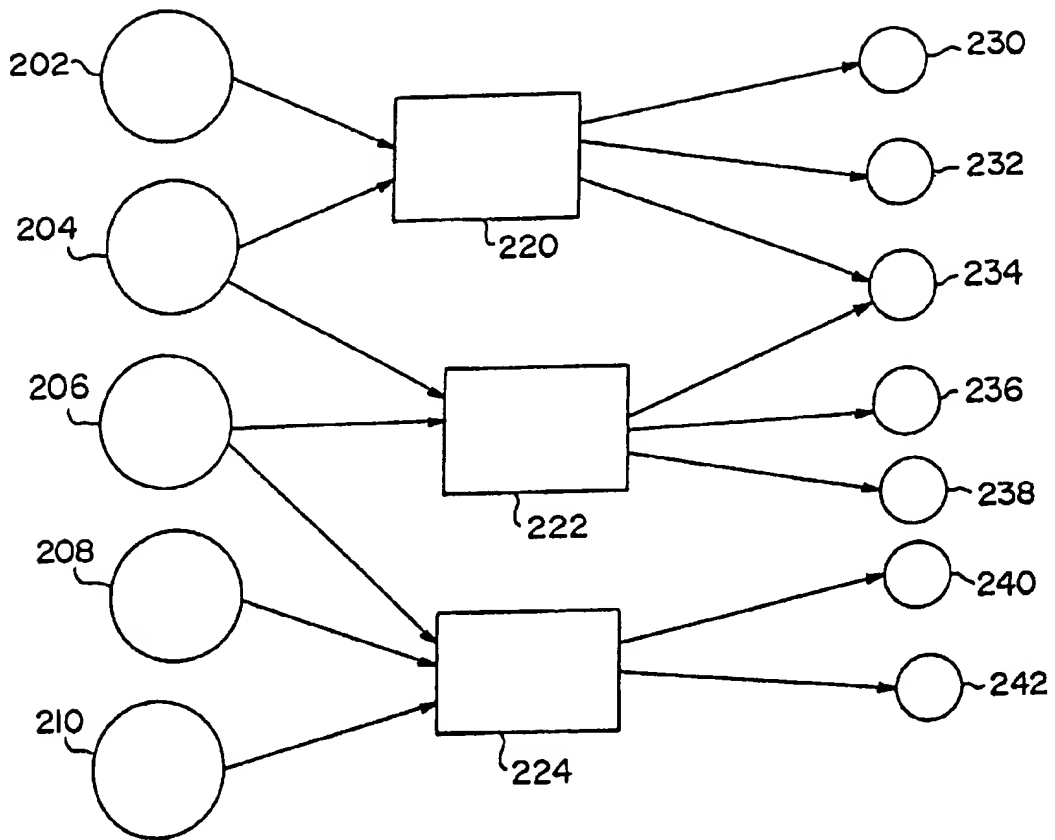


FIG. 2

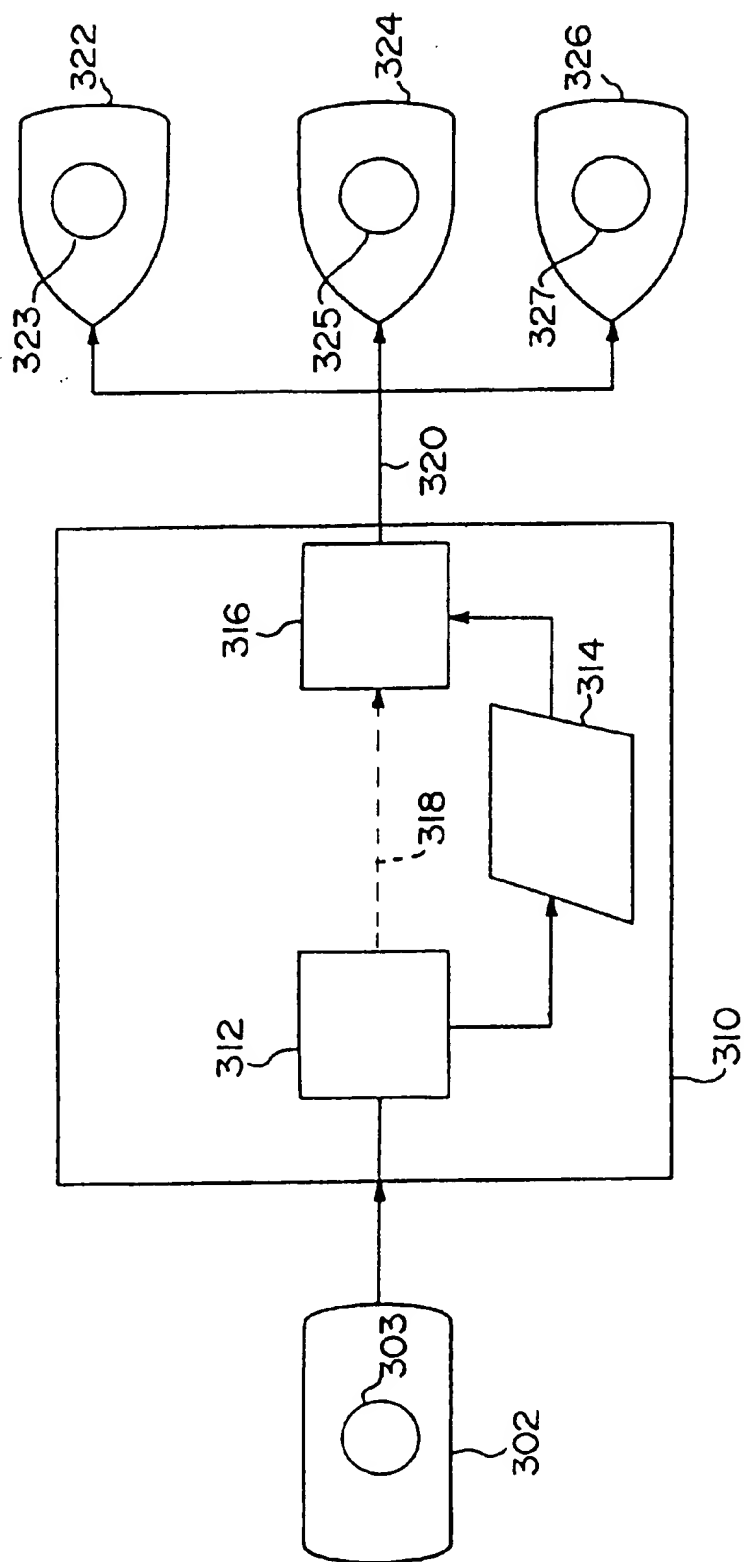


FIG. 3

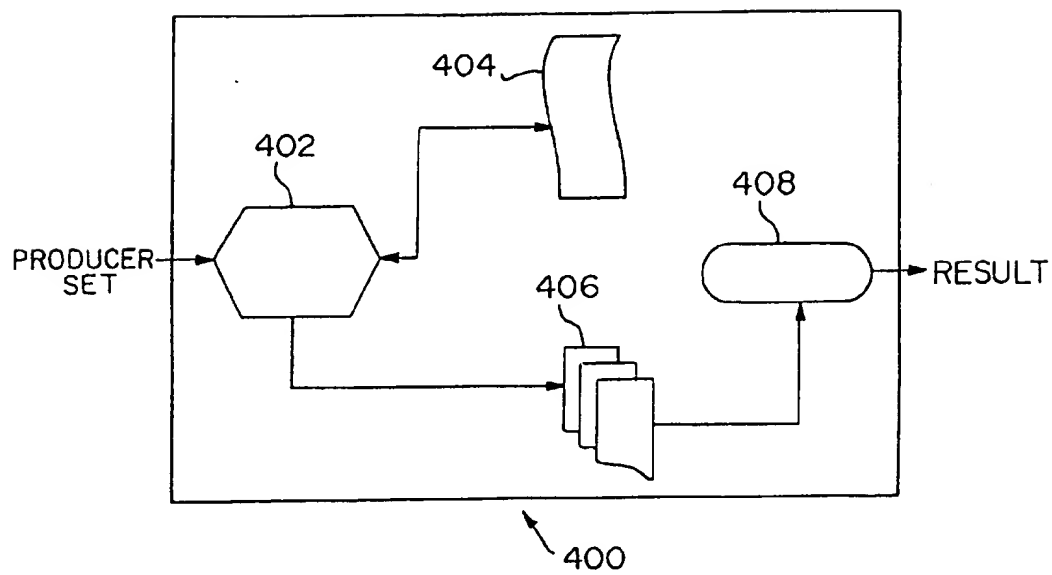


FIG. 4

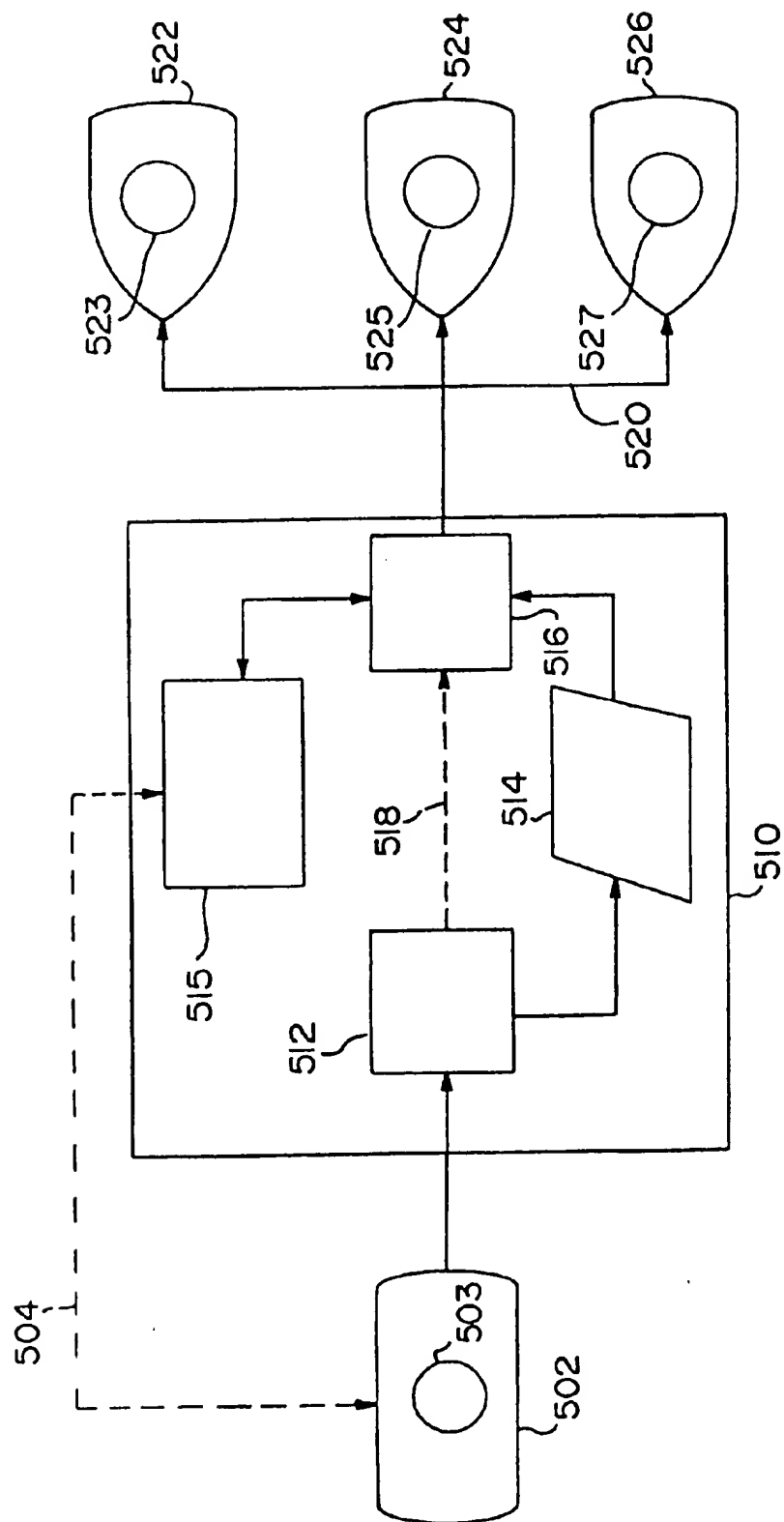


FIG. 5

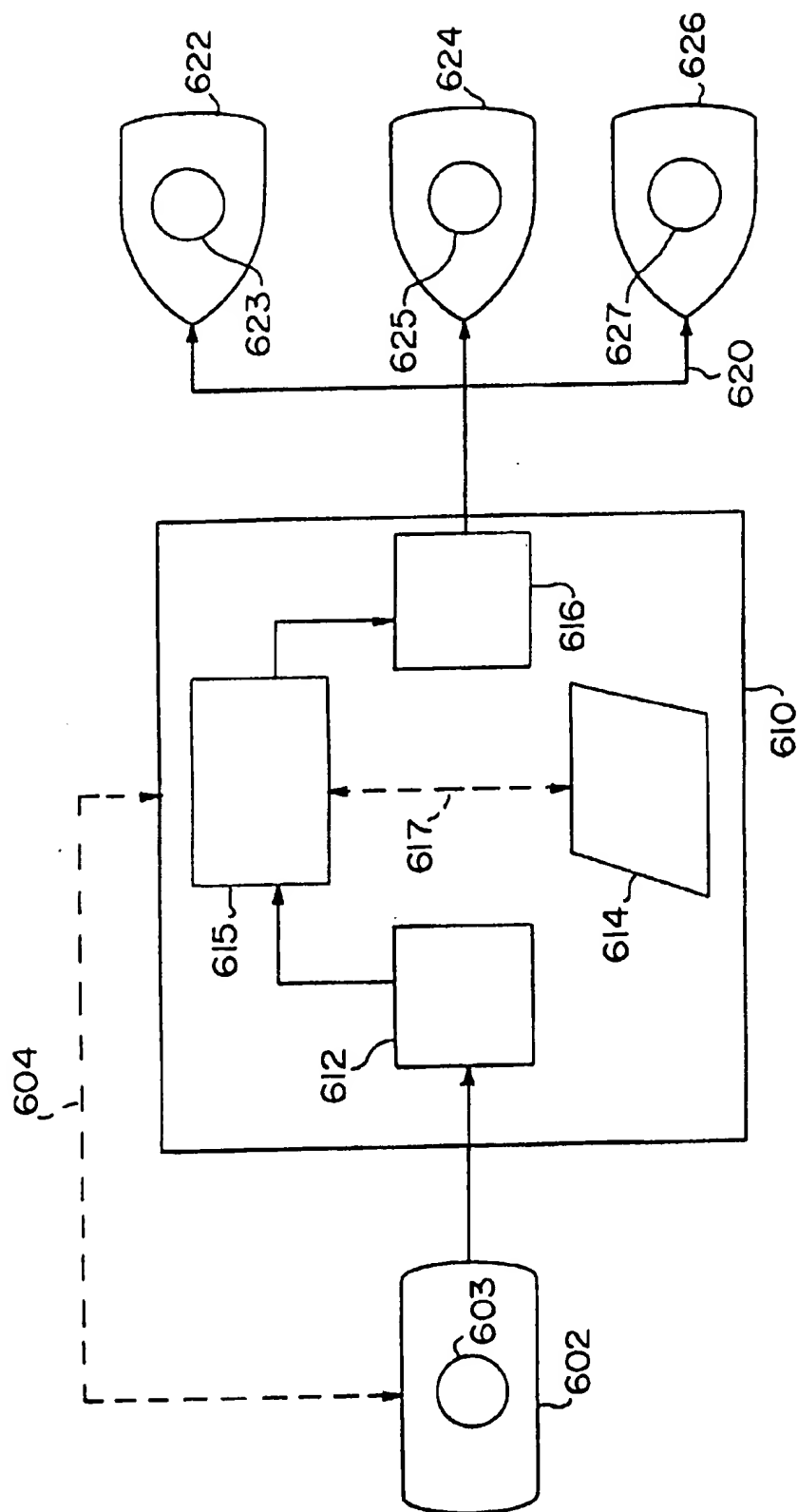


FIG. 6

1

WATCHDOG FOR TRUSTED ELECTRONIC CONTENT DISTRIBUTIONS

FIELD OF THE INVENTION

The present invention relates to electronic content distribution and more particularly to a computer watchdog system providing a secure communication channel. Specifically, a system is described for securing the distribution of electronic content from a producer, through a distributor, to a subscriber.

BACKGROUND OF THE INVENTION

Before proceeding it is helpful to define the following terms:

Content: any material that is possible to distribute electronically to consumers, such as, for example, advertisements, movies, recorded music, world wide web pages, or the like. Electronic content refers to material that may be distributed digitally, such as, for example, sampled music, digital video, or the like.

Producers: makers of content, such as, for example, an advertiser, an actor, a movie production company, a music production company, or the like.

Distributors: owners of communication channels, such as, satellite companies, cable-TV companies, telephone companies, Internet access providers, or the like.

Subscribers: members of the general public that are consumers of content, such as, individuals receiving cable-TV, individuals with access to the Internet, or the like.

Viewer: a device, such as, for example, a personal computer and/or work station, used to view content, visually as well as audibly.

Many producers of electronic content provide electronic content to various content distributors. The content distributors, in turn, select and route electronic content to subscribers. For example, a producer of electronic content may be an advertiser providing national advertisements to local cable-TV distributors. The local cable-TV heads, in turn, select national advertisements provided by the advertiser, insert these national advertisements into the local cable-TV programming, and provide the programming with the inserted advertisements to cable subscribers. FIG. 1 is a block diagram illustrating the distribution of advertisements from several advertisers 102, 104, and 106, through a content distributor 110, to subscribers 120, 122, 124, 126, and 128.

Payment agreements between a producer of content and a distributor of content depend on the content that is received by subscribers. The content received by subscribers may be classified as either "art" or "advertising". When the content received by subscribers is deemed "art" the content distributor pays the content producer per distribution of content to subscribers. When the content received by subscribers is deemed "advertising" the content producer pays the content distributor per distribution of content to subscribers.

For example, suppose video is the medium by which content is distributed. Pay-per-view movies in hotel rooms received via cable and/or satellite links is content that is deemed "art". In this case, the cable and/or satellite company is the content producer, the hotel is the distributor of pay-per-view movies, and subscribers, receiving these movies, are the hotel occupants. An example of video received by subscribers that is deemed "advertising" is the example given above in which a distributor selects and inserts national advertisements in local cable-TV programming.

2

In the case where the medium by which content is distributed is the world wide web, an example of content that is deemed "art" is a retail site offering digitized music for sale. In this case, the owner of the rights to the digitized music is the content producer, the owner of the retail site is the content distributor, and anyone with access to the Internet is a potential subscriber. An example of content distributed over the world wide web that is deemed "advertising" is advertisements appearing in on-line newspapers and/or magazines. In this case, the content producer is the advertiser, the distributor is the owner of the on-line magazine and/or newspaper, and a subscriber is anyone with access to the on-line magazine and/or newspaper. FIG. 2 is a block diagram illustrating the distribution of content from producers 202, 204, 206, 208, and 210, through distributors 220, 222, and 224, to subscribers 230, 232, 234, 236, 238, 240, and 242.

The infrastructure conventionally used to distribute content from producers, through distributors, to subscribers is shown in FIG. 3. FIG. 3 shows: a producer's site 302, a distributors site 310, content distribution channels 320, and subscriber's sites 322, 324, and 326. The producer's site 302 includes a preparation engine 303 for packaging electronic data in preparation for distribution. The distributors site 310 includes: a content receiver 312, a device for receiving content provided by a producer; a content archive 314, a device for storing data (e.g. digital music, video, and/or advertisements); a distribution engine 316, a mechanism for determining when and what content to distribute to a subscriber 322, 324, and/or 326 via the content distribution channels 320; and a bypass 318, for bypassing the content archive 314, sending content directly from the content receiver 312 to the distribution engine 316. Both the content receiver 312 and the distribution engine 316 may communicate with the content archive 314. The subscriber's sites 322, 324, and 326, each include a viewer for viewing multimedia data.

A fundamental difficulty with the distribution of content as illustrated in FIG. 3 is that in order to comply with the payment agreements between a producer of content and a distributor of content, a trustworthy measurement of the content received by subscribers is required. It may be possible to alter the distribution infrastructure to accommodate measurements of content received by subscribers. A measurement of content received by a subscriber may be, for example, the number of pay-per-view movies watched, the number of musical pieces downloaded from the Internet, and/or the number of times a particular on-line magazine was accessed. The content distributor may measure the content received by subscribers. Alternatively, meters may be introduced at subscriber sites in order to allow a content producer to measure content received by subscribers. In either case, the content producer and content distributor need to trust one another. Either the content producer or the content distributor may, through malice and/or by bungling, skew the measurement results. For example, with content deemed "advertising" the distributor may increase his revenue by pretending to distribute content to a large number of subscribers. Another example of fraud by content distributors, such as a TV or radio broadcasting company, occurs when the distributor miscalculates the residual royalties due performers (content producers) appearing in, for example, advertisements.

SUMMARY OF THE INVENTION

A computer watchdog system processes a producer set. The producer set is provided by a producer. The computer

3

watchdog comprises: a processing engine for creating a plurality of records of distribution content and for generating a plurality of reports based on the producer set; a distribution log for storing the plurality of records of distribution content; and an authenticated execution unit for validating a set of operations performed by the processing engine and transmitting an authenticating signal responsive to said set of operations being validated.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram illustrating the distribution of advertisements from an advertiser, through a content distributor, to subscribers.

FIG. 2 is a block diagram illustrating the distribution of content from producers, through distributors, to subscribers.

FIG. 3 is a block diagram which is helpful in understanding the infrastructure conventionally used to distributed content from producers, through distributors, to subscribers.

FIG. 4 is an illustration of an exemplary watchdog in accordance with an exemplary embodiment of the present invention.

FIG. 5 is a block diagram which illustrates an infrastructure used to distribute content from producers, through distributors, to subscribers in accordance with an exemplary embodiment of the present invention.

FIG. 6 is a block diagram which illustrates an infrastructure used to distribute content from producers, through distributors, to subscribers in accordance with an exemplary embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

Before proceeding it is helpful to define the following terms:

Computer watchdog system: a system that may be implemented in hardware, software or both for monitoring and controlling electronic content distributed from a producer, through distributors, to subscribers. The system enforces the just execution of distribution agreements between producers and distributors of content.

Records of distribution content: records that may include unique identifiers of the content. These records may also include information that a producer and/or a distributor may want to verify concerning the distribution of content. For example, the date and time the data had been received and/or distributed, the size of the data, the length (in time) of data transmission, the format of the content (e.g. TV transmission, music, or the like), the identity of the distributor, the identity of subscribers, and information relating to the customizing of data for both distributors and subscribers, may be included in the records.

Distribution log: a log containing records of distribution content.

Processing Engine: a computer including a central processing unit, a memory, and an input/output interface.

Archive: a device for storing data.

Authenticated execution unit: cryptographic means allowing the watchdog to determine the validity of programs, that either reside in the watchdog or are sent to the watchdog by a producer or by a distributor, to be executed by the processing engine. Once validity is established the watchdog may authenticate the operations performed by the processing engine to a producer or distributor at a remote location.

Reports: include information ranging from the entire contents of the distribution log, to a subset of the informa-

4

tion that is requested, by a producer and/or a distributor, from a computer watchdog system. For example, a report may include all pertinent information regarding one particular piece of data that the producer sent to the distributor; e.g. content X received by distributor Y, content X archived at Z time, content X distributed to subscriber S, content X removed from archive.

Tamper protection: any mechanism for protecting against unauthorized access to the information stored in, and the operation of the computer watchdog system. Tamper protection may include logic and other circuitry to detect, for example, temperature and voltage changes that are outside of a pre-specified operating range. The presence of X-rays, and/or physical intrusion (e.g. mesh intrusion) through the outer layers (skin) of the watchdog, may also be detected.

The safety and security of distribution of content from a producer, through distributors, to subscribers may be enforced by a computer watchdog system. A computer watchdog system may be installed at the distributors site or location. The watchdog will monitor and control information related to the distribution of content, provided by a producer, and delivered (distributed) to subscribers by the distributor. The watchdog may thus serve as an agent that is trusted by both producers and distributors. The processing operations of the watchdog facilitate the implementation of agreements between a producer and a distributor, by providing each with relevant trustworthy information concerning content and its distribution. The watchdog may be designed to carry out the monitoring and control operations justly while resisting exogenous attempts at tampering.

An exemplary watchdog 400 in accordance with a first embodiment of the present invention is shown in FIG. 4. The watchdog 400 includes: a processing engine 402, a distribution log 404, and an authenticated execution unit 408. The processing engine 402 receives a producer set provided by a producer. The processing engine 402 creates a plurality of records of distribution content from the producer set. These records may be stored in the distribution log 404. By processing the records of distribution content, and the information stored in the log 404, the processing engine 402 may generate a plurality of reports 406 containing pertinent information.

For example, a producer set may contain formatted and electronically packaged data that the producer has sent to a distributor, as well as information that a producer wishes the watchdog to store in a distribution log. Such electronically packaged data may contain, for example, a TV advertisement, as well as a time-stamp that indicates the time the advertisement was sent to the distributor, and the size of the advertisement. Records of distribution content such as a time-stamp and size information allow a watchdog to report to a producer the length of time it take the distributor to receive data, and to verify that all the data had been received by the distributor. A processing engine may parse the data to create and log such records of distribution content in the distribution log. Furthermore, the processing engine may, accessing the log, generate a plurality of reports containing information that is pertinent to the producer and/or distributor.

The distribution log 404 contains records of the content, of a producer set, received and/or distributed by a distributor. These records of distribution content may include unique identifiers of the content. The records may also include information that a producer and/or a distributor may want to verify concerning the distribution of content. For example, the date and time the data had been received and/or

distributed, the size of the data, the length (in time) of data transmission, the format of the content (e.g. TV transmission, music, or the like), the identity of the distributor, the identity of subscribers, and information relating to the customizing of data for both distributors and subscribers, may be included in the records.

The plurality of reports 406 may include information ranging from the entire contents of the distribution log, to a subset of the information that is requested, by a producer and/or a distributor, from the watchdog 400. For example, one report of the plurality of reports 406 may include all pertinent information regarding one particular piece of data that the producer sent to the distributor; e.g. content X received by distributor Y, content X archived at Z time, content X distributed to subscriber S, content X removed from archive.-

The authenticated execution unit 408 may be implemented in software that resides in the watchdog 400. The authenticated execution unit 408 lends the watchdog 400 the capability to determine the validity of programs, that either reside in the watchdog 400 or are sent to the watchdog 400 by a producer or by a distributor, to be executed by the processing engine 402. Hence, the authenticated execution unit 408 may prevent unauthorized software from being run by the watchdog 400. The authenticated execution unit 408 may also prevent the counterfeiting and/or forgery of the watchdog 400 by a device attempting to masquerade as the watchdog 400. The operations performed by the processing engine 402 may be validated by the authenticated execution unit 408 by verifying a digital signature against a certificate containing a cryptographic key. Hence, the watchdog may authenticate the operations performed by the processing engine to a producer or distributor at a remote location. For example, an authenticated execution unit may include the ability to control when and how the watchdog 400 receives software updates, and the ability to authenticate messages from the watchdog 400 to a remote device.

A trustworthy watchdog may be designed to be resistant to exogenous tampering. Tamper protection may include logic and other circuitry to detect, for example, temperature and voltage changes that are outside of a pre-specified operating range. The presence of X-rays, and/or physical intrusion (e.g. mesh intrusion) through the outer layers (skin) of the watchdog, may also be detected. The watchdog may respond to an attempt at tampering by "zero-izing" (erasing) memory that is otherwise non-volatile. The memory to be "zero-ized" when a tampering attempt is sensed, may contain secret cryptographic keys and other information that allows a watchdog to authenticate itself and the resident software. In other words, tamper protection renders some subset of the memory unavailable, either by destroying it ("zero-ization") or by making it physically unavailable. "Zero-ization" may not destroy the contents of a watchdog's memory, but rather destroy the ability of a watchdog to (cryptographically) prove that it is authentic. For example, tamper protection employed by a watchdog may be designed to meet or exceed the requirements of the US government's FIPS 140-1 standard for a level 4 cryptographic module. Tamper protection prevents unauthorized access to the contents of a watchdog.

A watchdog with tamper protection may be referred to as an untampered device. An un-tampered device is a watchdog that is able to authenticate itself to a producer, for example, as a valid watchdog, running authenticated software; i.e. all secret cryptographic keys and information are intact. A computer watchdog system as described in the foregoing may be implemented, for example, using the IBM 4758

cryptographic coprocessor executing software that may be developed using IBM 4758's OEM development environment.

The infrastructure used to distribute content from producers, through distributors, to subscribers in accordance with another embodiment of the present invention is shown in FIG. 5. FIG. 5 shows: a producer's site 502, a distributors site 510, content distribution channels 520, and subscriber's sites 522, 524, and 526. The producer's site 502 includes a preparation engine 503, for packaging electronic data in preparation for distribution. The distributors site 510 includes: a watchdog 515, a content receiver 512, a device for receiving content provided by a producer; a content archive 514, a device for storing data (e.g. digital music, video, and/or advertisements); a distribution engine 516, a mechanism for determining when and what content to distribute to a subscriber 522, 524, and/or 526 via the content distribution channels 520; and a bypass 518, for bypassing the content archive 514, sending content directly from the content receiver 512 to the distribution engine 516. Both the content receiver 512 and the distribution engine 516 may communicate with the content archive 514. The watchdog 515 communicates with the distribution engine 516. The subscriber's sites 522, 524, and 526, each include a viewer for viewing multimedia data. FIG. 5 also shows a watchdog-producer loop 504. The loop 504 is a communication path through which a producer may query the watchdog 515 concerning the verification of information in the plurality of reports generated by the watchdog 515.

Once content has been packaged by the preparation engine 503 at the producer's site the producer sends a producer set to a distributor. The producer set is received by the content receiver 512. The distribution content of the producer set may then be stored in the content archive until a decision is made to distribute the content. Alternatively, the distribution content may be forwarded directly to the distribution engine 516 using the bypass 518. Once the decision is made to distribute content the distribution engine 516 notifies the watchdog 515 of the content to be distributed. The watchdog 515 may then log all the information that is relevant to the current distribution of content. The distribution content is then distributed to subscribers 522, 524, and/or 526, via the content distribution channels 520. The subscribers 522, 524, and/or 526, receive the content or data.

In variation to the embodiment, in accordance with the present invention, shown in FIG. 5, an infrastructure to distribute content from producers, through distributors, to subscribers as shown in FIG. 6 may be used. The distributors site 610 includes: a watchdog 615, a content receiver 612, a device for receiving content provided by a producer; a content archive 614, a device for storing data (e.g. digital music, video, or advertisements); a distribution engine 616, a mechanism for determining when and what content to distribute to a subscriber 622, 624, and/or 626 via the content distribution channels 620; and a communication bus 617, linking the watchdog 615 and the content archive 614. Both the content receiver 612 and the distribution engine 616 communicate with the watchdog 615. The watchdog 615 communicates with the content archive 614.

The infrastructure for distributing content from producers, through distributors, to subscribers shown in FIGS. 5 and 6 may be used in conjunction with a trusted watchdog (515, 615, respectively) performing not only passive monitoring, but active interception and processing of a producer set as well. The watchdog 615 of FIG. 6, is shown communicating with the content archive 614 via the communication bus 617. Hence, the watchdog 615 may access any data (e.g. digital

music, movies, and/or advertisements) that is intended for distribution and subsequent receipt by subscribers. The contents of the content archive, however, may not be protected from tampering. Though the watchdog may discern if anything in the content archive had been tampered with, the watchdog may not be able to prevent such tampering. Therefore, for purposes of security, data, information, and/or programs stored in the content archive may be analyzed by the watchdog. Additionally, the watchdog may absorb, fully or partially, the functionality of the distribution engine, thus increasing the flexibility of the watchdog in monitoring and controlling the flow of data from distributor to subscriber.

The producer prepares a producer set. The producer set may include: raw data, to be transformed into distribution content, a distribution selection program for selecting distributor specific information from the data, and a distributor transformation program for processing the data for receipt by a distributor. The distributor transformation program prepares a distributor set. The distributor set may include: raw data, to be transformed into content for a subscriber, a subscriber selection program, for selecting subscriber specific information from the data, and a subscriber transformation program for customizing the data sent to individual subscribers.

The watch dog receives a producer set, logs the receipt, and executes the distribution selection program to determine if a particular distributor is to receive the data. The watchdog may store some of the data of the producer set in the content archives. For example, an advertisement may be packaged by a producer for a particular retail chain store with information that specifies that the advertisement applies only to store locations in a pre-specified area. The selection program determines if a particular distributor is in the pre-specified area or not, and whether or not to distribute the advertisement to subscribers.

If a distributor is to receive the data, the watchdog executes the distributor transformation program to prepare content for the distributor's site. If the transformation is successful the watchdog may store some information or data in a content archive and retain some information or data internally. An unsuccessful transformation may take several forms, including: content not meant for distribution to a particular distributor and/or an associated set of subscribers, incorrect content, and unsecure program(s) included in the data. In case of an unsuccessful transformation the watchdog may log the event and/or discard the data, possibly notifying the producer and/or the distributor of the failure.

The distribution engine, or alternatively the watchdog, decides when some content is to be distributed, and the watchdog selects and executes a subscriber selection program. The watchdog may retrieve data and information stored in the content archive. The decision to distribute content may be based on several inputs. For example, the time and date, expiration of content and/or subscriber selection programs, and stored records of distribution content. The watchdog then executes a subscriber transformation program. Both distributor and subscriber transformation programs customize data for the particular use of subscribers. These transformation programs may control, for example, the language of a voice/sound track to be distributed, depending on the ethnic makeup of the target subscribers. These programs may additionally control, for example, the volume level of the voice/sound track to be distributed to subscribers, depending on factors like the age group of the subscribers. Note that selection and transformation programs may be internal to a watchdog, loaded into a watchdog, and/or stored in a content archive. Furthermore,

the distribution log may contain information describing what selection and transformation programs were applied to which content.

The selection programs may use information that is fed-back to a distributor's site from subscriber sites. This information feedback may be used by the watchdog to customize distribution content. For example, if a subscriber is searching the Internet for information about running, a watchdog may select advertisements (content) for the subscriber (for insertion in the Web pages viewed by the subscriber) that are related to running; e.g. advertisements for running shoes.

The following table illustrates some examples of transformation and selection for both the art and advertising categories of content.

	Art	Advertising
Distributor Selection	Select which hotels of a chain of hotels are to receive what set of movies. Shut off access to movies for hotels that have not paid the producer.	Select which cable-TV companies are to receive what set of advertisements. Block transmission of particular advertisements to particular cable-TV companies.
Distributor Transformation	Embed cryptographic watermark in movies based on a hotel's identity.	Change the language of an advertisement depending on the distributor's location.
Subscriber Selection	Authenticate a subscriber by verifying a digital signature against a certificate containing a public encryption key.	Change advertisement sent to subscriber based on the time of day. Block advertisements for producers who have not paid distributor.
Subscriber Transformation	Embed subscriber and distributor identifies in a cryptographic watermark.	Resolve contention between two advertisers competing for one slot. Change set of goods advertised by a retailer based on an inferred interest (e.g. referrer field, cookies, content of Web page) of a subscriber.

To communicate to a watchdog whether or not content had actually reached the subscriber in the appropriate demographic class, and/or whether content had reached a subscriber at all, a watchdog computer system may be equipped with watchpuppies. The watchpuppies are trusted devices residing in subscriber's sites. Watchpuppies installed in all or some of the subscriber sites may work in concert with a watchdog installed at a distributors site. The watchpuppies may further provide information that is helpful in distinguishing subscribers that are human from subscribers that are automatons, e.g. web search engines. In addition, the watchpuppies may assist in monitoring user-to-cached-copy interactions of subscribers as well as server-to-cache interactions. A watchdog puppy may be implemented by, for example, the IBM 4758 cryptographic coprocessor, IBM MultiFunction Card (IBM MFC 4.0 smart card), as well as smart cards from Schlumberger and other vendors, such as smart cards supporting standards for security cards like the ISO-7816 set of standards. Alternatively, subscriber sites may be provided with all of the functionality of a computer watchdog system.

A watchdog may embed data intended for a watchdog puppy, into the content to be distributed. The watchdog puppy may then

scan all incoming content for such embedded data and log the receipt of the data. Hence, the watchdog may verify that distributed content was actually received by subscribers. A channel between the distributor and the subscriber may be secured by utilizing a security protocols for communications between a watchdog and a watchdog. A security protocol such as, for example, IPSEC, see RFC 1825: Security Architecture for the Internet Protocol, Naval Research Lab, August 1995, RFC 1826: IP Authentication Header, Naval Research Lab, August 1995, RFC 1827: IP Encapsulating Security Payload (ESP), Naval Research Lab, August 1995; SSL, see The SSL Protocol, by K. E. B Hickman (developed by Netscape Communications Corporation), December 1995, The IETF's internet draft: HTTP Over TLS, dated March 1998; or the like may be used. Such a protocol may be more secure than a software-only implementation, because of the tamper resistant nature of the watchdog and watchdog. Moreover, the implementation of a security protocol may result in better performance due to hardware acceleration of cryptographic algorithms within the watchdog and watchdog.

Although illustrated and described herein with reference to certain exemplary embodiments, the present invention is nevertheless not intended to be limited to the details shown. Rather, various modifications may be made in the details within the scope and range of equivalents of the claims and without departing from the spirit of the invention.

What is claimed:

1. A computer watchdog system for processing a producer set provided by a producer, the computer watchdog comprising:

- a processing engine for creating a plurality of records of distribution content and for generating a plurality of reports based on the producer set;
- a distribution log for storing the plurality of records of distribution content;
- an authenticated execution unit for validating a set of operations performed by the processing engine and transmitting an authenticating signal responsive to said set of operations being validated; and
- tamper protection means for detection of unauthorized access to the computer watchdog system by detecting one of a plurality of tamper indicators, wherein the plurality of tamper indicators include at least one of: temperature change, voltage change, presence of X-rays, physical intrusion.

2. A computer watchdog system as recited in claim 1, wherein the processing engine includes means for preparing a distributor set by selectively transforming the producer set.

3. A computer watchdog system as recited in claim 2, wherein the processing engine includes means for customizing the distributor set by selectively transforming the distributor set into subscriber data.

4. A computer watchdog system as recited in claim 1, further comprising a watchdog for verifying ones of the plurality of records of distribution content.

5. A computer watchdog system as recited in claim 1, wherein the plurality of records of distribution content each include a unique identifier of content.

6. A computer watchdog system as recited in claim 1, wherein the plurality of records of distribution content each include at least one of: time of data receipt, date of data receipt, size of data, length of data transmission, format of content, identity of distributor, identity of subscribers.

7. A computer watchdog system as recited in claim 1, further comprising tamper protection for preventing unau-

thorized access to the computer watchdog system by modifying portions of system memory.

8. A computer watchdog system as recited in claim 1, wherein each of the plurality of reports include at least one of the plurality of records of distribution content stored in the distribution log.

9. A computer watchdog system as recited in claim 1, wherein each of the plurality of reports include at least one of: time of data receipt, date of data receipt, size of data, length of data transmission, format of content, identity of distributor, identity of subscribers.

10. A computer watchdog system as recited in claim 1, wherein the producer set includes: data, at least one of a plurality of distributor selection instructions, at least one of a plurality of distributor transformation instructions.

11. A computer watchdog system as recited in claim 10, wherein ones of the plurality of distributor selection instructions selects ones of a plurality of distributors based on data included in the producer set.

12. A computer watchdog system as recited in claim 10, wherein ones of the plurality of distributor transformation instructions embed a cryptographic watermark in data included in the producer set.

13. A computer watchdog system as recited in claim 10, wherein ones of the plurality of distributor transformation instructions produce at least one of: subscriber data, at least one of a plurality of subscriber selection instructions, at least one of a plurality of subscriber transformation instructions.

14. A computer watchdog system as recited in claim 13, wherein ones of the plurality of subscriber selection instructions authenticate a subscriber by verifying a digital signature against an encryption key.

15. A computer watchdog system as recited in claim 13, wherein ones of the plurality of subscriber transformation instructions embed subscriber and distributor identities in a cryptographic watermark.

16. A method of processing a producer set provided by a producer to a distributor for distribution to a subscriber, comprising the steps of:

- locating at the distributor's location a computer watchdog system for:
- creating a plurality of records of distribution content;
- generating a plurality of reports based on the producer set;
- storing the plurality of records of distribution content;
- validating a set of operations performed on the producer set;
- transmitting an authenticating signal to the producer on a watchdog-producer communication loop if said set of operations are validated; and
- detecting unauthorized access to the computer watchdog by being responsive to a plurality of tamper indicators which include at least one of temperature change, presence of X-rays, and physical intrusion.

17. A method of processing a producer set according to claim 16, further comprising the step of preparing a distributor set by selectively transforming the producer set.

18. A method of processing a producer set according to claim 17, further comprising the step of customizing the distributor set by selectively transforming the distributor set into subscriber data.

19. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for processing a producer set provided by a producer to a distributor for distribution to a subscriber, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer watchdog to effect:

11

- (a) creating a plurality of records of distribution content;
- (b) generating a plurality of reports based on the producer set;
- (c) storing the plurality of records of distribution content;
- (d) validating a set of operations performed on the producer set;
- (e) transmitting an authenticating signal if said set of operations are validated; and
- (f) providing tamper protection for detecting unauthorized access to the computer watchdog by being responsive to a plurality of tamper indicators including at least one of temperature change, presence of X-rays, and physical intrusion.

20. An article of manufacture as recited in claim 19, the computer readable program code means in said article of manufacture further comprising computer readable program code means for causing a computer to effect:

preparing a distributor set by selectively transforming the producer set.

21. An article of manufacture as recited in claim 20, the computer readable program code means in said article of manufacture further comprising computer readable program code means for causing a computer to effect:

customizing the distributor set by selectively transforming the distributor set into subscriber data.

22. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing processing a producer set provided by a producer to a distributor for distribution to a user, the computer readable program code means in said computer program product comprising computer readable program code means for causing a watchdog computer located at the distributor's location to effect:

- (a) creating a plurality of records of distribution content;
- (b) generating a plurality of reports based on the producer set;
- (c) storing the plurality of records of distribution content;
- (d) validating a set of operations performed on the producer set;
- (e) transmitting in response to a producer query an authenticating signal on a watchdog-producer communication loop if said set of operations are validated; and
- providing tamper protection for detection of unauthorized access to the computer watchdog by being responsive to a plurality of tamper indicators including at least one of temperature, change, presence of X-rays and physical intrusion.

23. A computer program product as recited in claim 22, the computer readable program code means in said computer program product further comprising computer readable program code means for causing a computer to effect:

preparing a distributor set by selectively transforming the producer set.

24. A computer program product as recited in claim 23, the computer readable program code means in said computer program product further comprising computer readable program code means for causing a computer to effect:

customizing the distributor set by selectively transforming the distributor set into subscriber data.

25. A storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for processing a producer set provided by a producer to a distributor for distribution to a subscriber, said method comprising the steps of:

12

- (a) creating a plurality of records of distribution content;
- (b) generating a plurality of reports based on the producer set;
- (c) storing the plurality of records of distribution content;
- (d) validating a set of operations performed on the producer set;
- (e) transmitting an authenticating signal if said set of operations are validated; and
- (f) providing tamper protection for the detection of unauthorized access to the computer watchdog by being responsive to a plurality of tamper indicators including at least one of temperature change, presence of X-rays and physical intrusion.

26. A computer watchdog system for processing a set of advertisements provided by an advertiser and distributed by a distributor, characterized by a computer watchdog located at the distributor's site comprising:

- a processing engine for creating a plurality of records of distributed advertisements and for generating a plurality of reports based on the set of advertisements;
- a distribution log for storing the plurality of records of distributed advertisements;
- an authenticated execution unit for validating a set of operations performed by the processing engine and transmitting an authenticating signal responsive to said set of operations being validated;
- a watchdog-producer communication loop through which the producer may query the watchdog; and
- tamper protection to detect unauthorized access to the computer watchdog by being responsive to a plurality of tamper indicators.

27. A computer watchdog system as recited in claim 26, wherein the processing engine includes means for preparing a cable TV distribution set by selecting ones of the set of advertisements and changing the language of ones of the set of advertisements.

28. A computer watchdog system for processing a producer set provided by a producer to a distributor for distribution to a user, characterized by a computer watchdog at the distributor's location comprising:

- a processing engine for creating a plurality of records of distribution content and for generating a plurality of reports based on the producer set;
- a distribution log for storing the plurality of records of distribution content;
- an authenticated execution unit for validating a set of operations performed by the processing engine and transmitting an authenticating signal responsive to said set of operations being validated; and
- tamper protection logic for detecting unauthorized access to the computer watchdog system by detecting one of a plurality of tamper indicators, wherein the plurality of tamper indicators include at least one of: temperature range, voltage change, presence of X-rays, physical intrusion.

29. In a computer watchdog system for processing a producer set provided by a producer to a distributor for distribution to a user characterized by, a computer watchdog at the distribution location comprising:

- a processing engine for creating a plurality of records of distribution content and for generating a plurality of reports based on the producer set;
- a distribution log for storing the plurality of records of distribution content;

13

an authenticated execution unit for validating a set of operations performed by the processing engine that either reside in the computer watchdog system or are sent to the computer watchdog system by the producer or by a distributor, and transmitting an authenticating signal responsive to said set of operations being validated;

14

a watchdog-producer communication loop through which the producer can query the watchdog; and
tamper protection logic responsive to unauthorized access to the computer watchdog.

* * * * *



US006289318B1

(12) **United States Patent**
Barber(10) **Patent No.:** **US 6,289,318 B1**
(45) **Date of Patent:** **Sep. 11, 2001**(54) **METHOD AND ARCHITECTURE FOR
MULTI-LEVEL COMMISSIONED
ADVERTISING ON A COMPUTER
NETWORK**(76) **Inventor:** **Timothy P. Barber, 11931 Chalon La.,
San Diego, CA (US) 92128**(*) **Notice:** Subject to any disclaimer, the term of this
patent is extended or adjusted under 35
U.S.C. 154(b) by 0 days.(21) **Appl. No.:** **09/275,696**(22) **Filed:** **Mar. 24, 1999****Related U.S. Application Data**(60) **Provisional application No. 60/079,223, filed on Mar. 24,
1998.**(51) **Int. Cl.⁷** **G06F 17/60**(52) **U.S. Cl.** **705/14**(58) **Field of Search** **705/14, 26, 40;
235/380, 384; 707/2, 5**(56) **References Cited****U.S. PATENT DOCUMENTS**

5,537,314	*	7/1996	Kanler	705/14
5,666,416		9/1997	Micali	380/23
5,677,955		10/1997	Doggett et al.	380/24
5,708,780		1/1998	Levergood et al.	395/200.12
5,715,314		2/1998	Payne et al.	380/24
5,724,424		3/1998	Gifford	380/24
5,897,621		4/1999	Boesch et al.	705/26
5,991,740	*	11/1999	Messer	705/27
6,014,635	*	1/2000	Harris et al.	705/14
6,029,150	*	2/2000	Kravitz	705/39
6,092,053	*	7/2000	Boesch et al.	705/26
6,128,599	*	10/2000	Walker et al.	705/14

FOREIGN PATENT DOCUMENTS

WO 00/77691 * 12/2000 (WO) 705/14

OTHER PUBLICATIONS

"SubScrip—An efficient protocol for pay-per-view pay-
ments on the Internet," Andreas Furche & Graham Wright-
son, Dept. of Computer, Science, U. of Newcastle, Oct. 16,
1996.

"PayWord and MicroMint: Two simple micropayment
schemes," Ronald L. Rivest* and Adi Shamir**, *MIT
Laboratory for Computer Science, **Weizmann Institute of
Science, May 7, 1996, pp. 1-18.

"iKP—A Family of Secure Electronic Payment Protocols,"
IBM Research, Mar. 15, 1995 pp. 1-17.

"Mini-Pay: Charging per Click on the Web," IBM
Research-Haifa Research Lab-Tel-Aviv Annex Apr. 10,
1997, pp 1-20.

"Millicent: Frequently Asked Questions," Apr. 15, 1997, pp.
1-3.

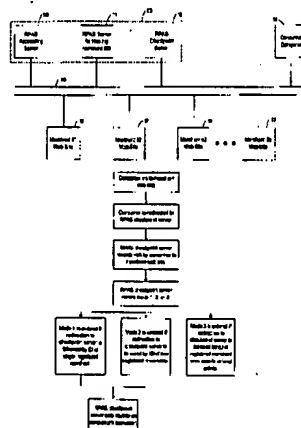
"Millicent-specific elements for an HTTP payment proto-
col," Apr. 15, 1997, pp 1-8.

"The State of the Art in Electronic Payment Systems," N.
Asokan et al, *Computer*, Sep. 1997, pp. 28-35.

(List continued on next page.)

Primary Examiner—Stephen Gravini(74) **Attorney, Agent, or Firm**—Ware, Fressola, Van Der
Sluys & Adolphson, LLP(57) **ABSTRACT**

A method and architecture for rewarding a merchant that
operates a server on a computer network, and in particular
on the Internet, when a consumer accesses the server and
later access a server of a paying merchant, i.e. a merchant
who has agreed to provide a reward to one or more of the
merchants the consumer accessed on the way, in tracing a
course through the network, to accessing the paying mer-
chant. The invention involves having a service operate
servers, on the computer network, that automatically dis-
tribute any reward provided by a paying merchant. The
method is not intended to reward all merchants visited by a
consumer on the way to a paying merchant; it distributes
rewards only approximately, trading off accuracy for a lower
burden of computation.

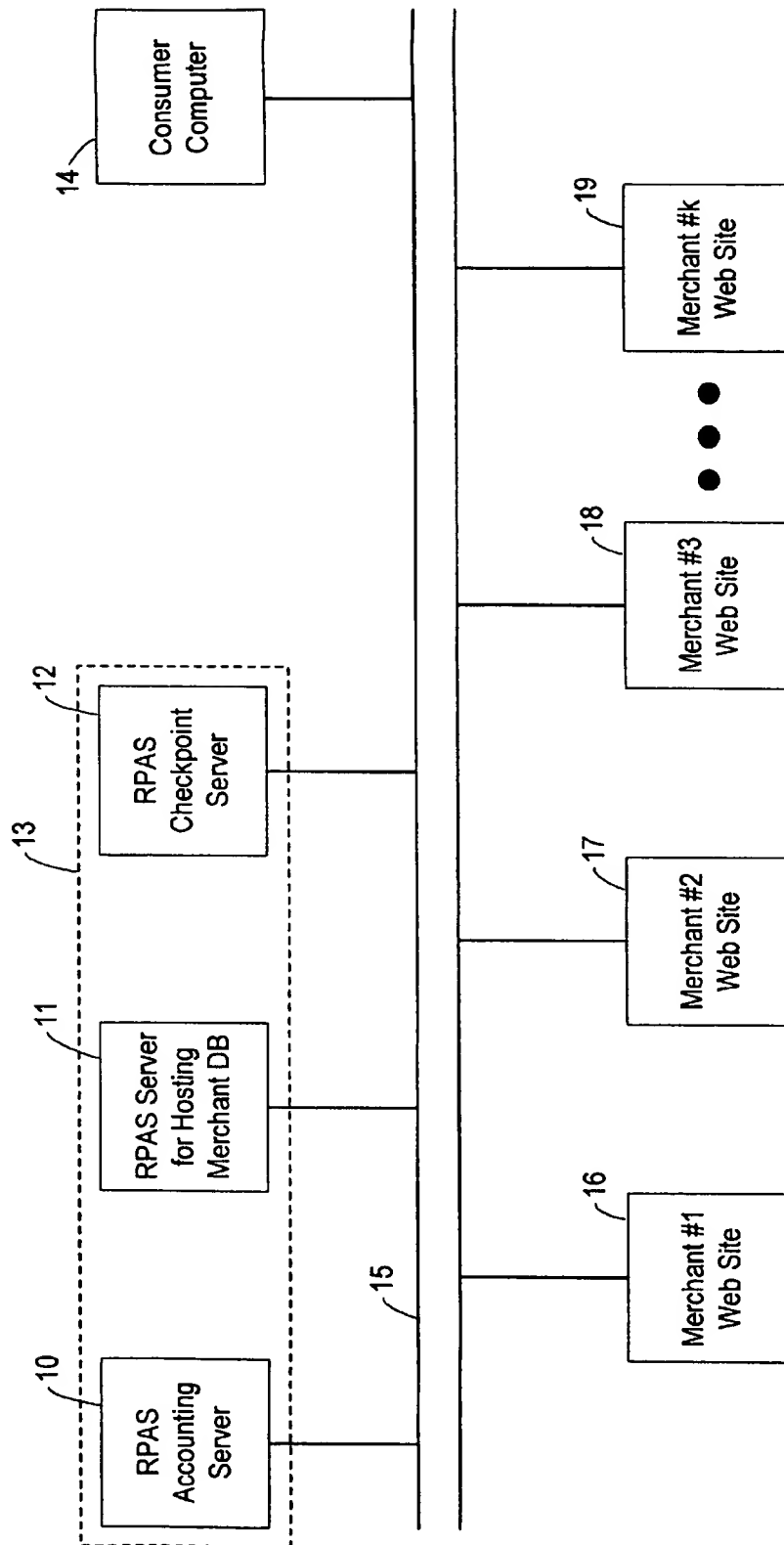
9 Claims, 3 Drawing Sheets

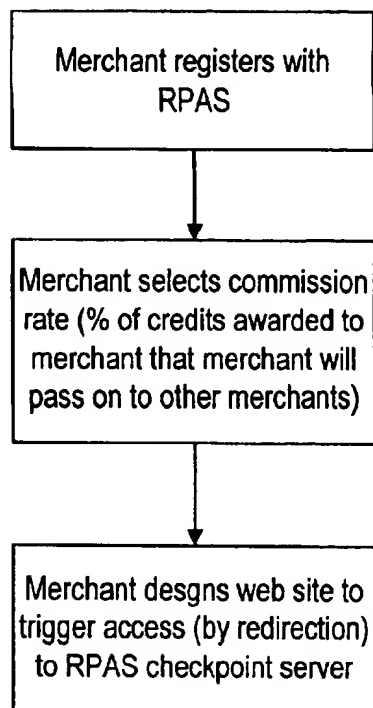
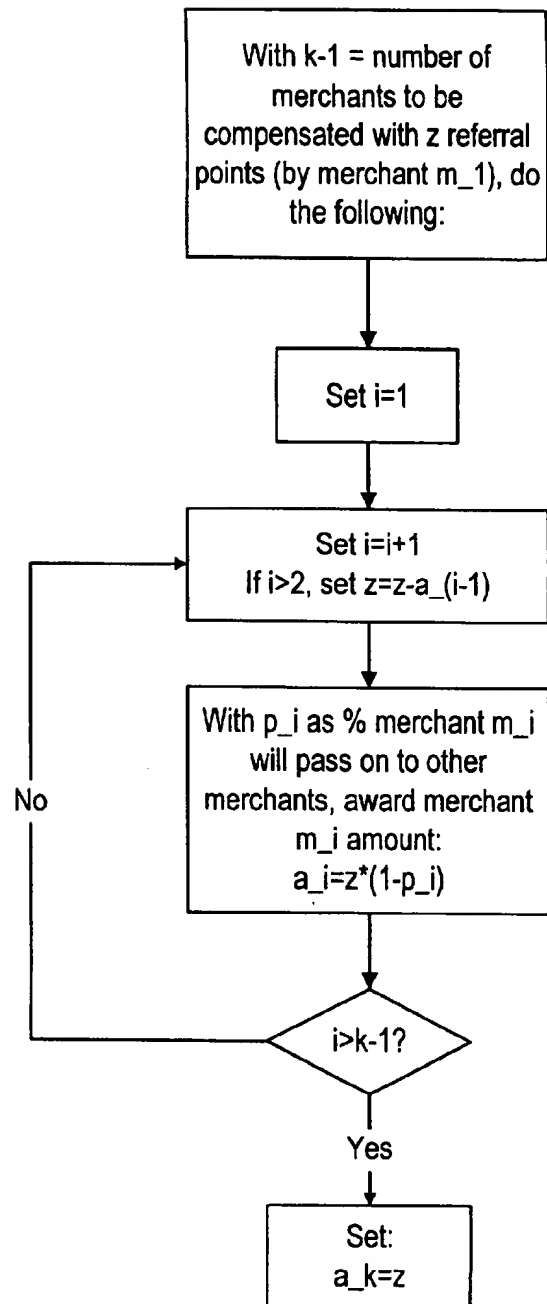
OTHER PUBLICATIONS

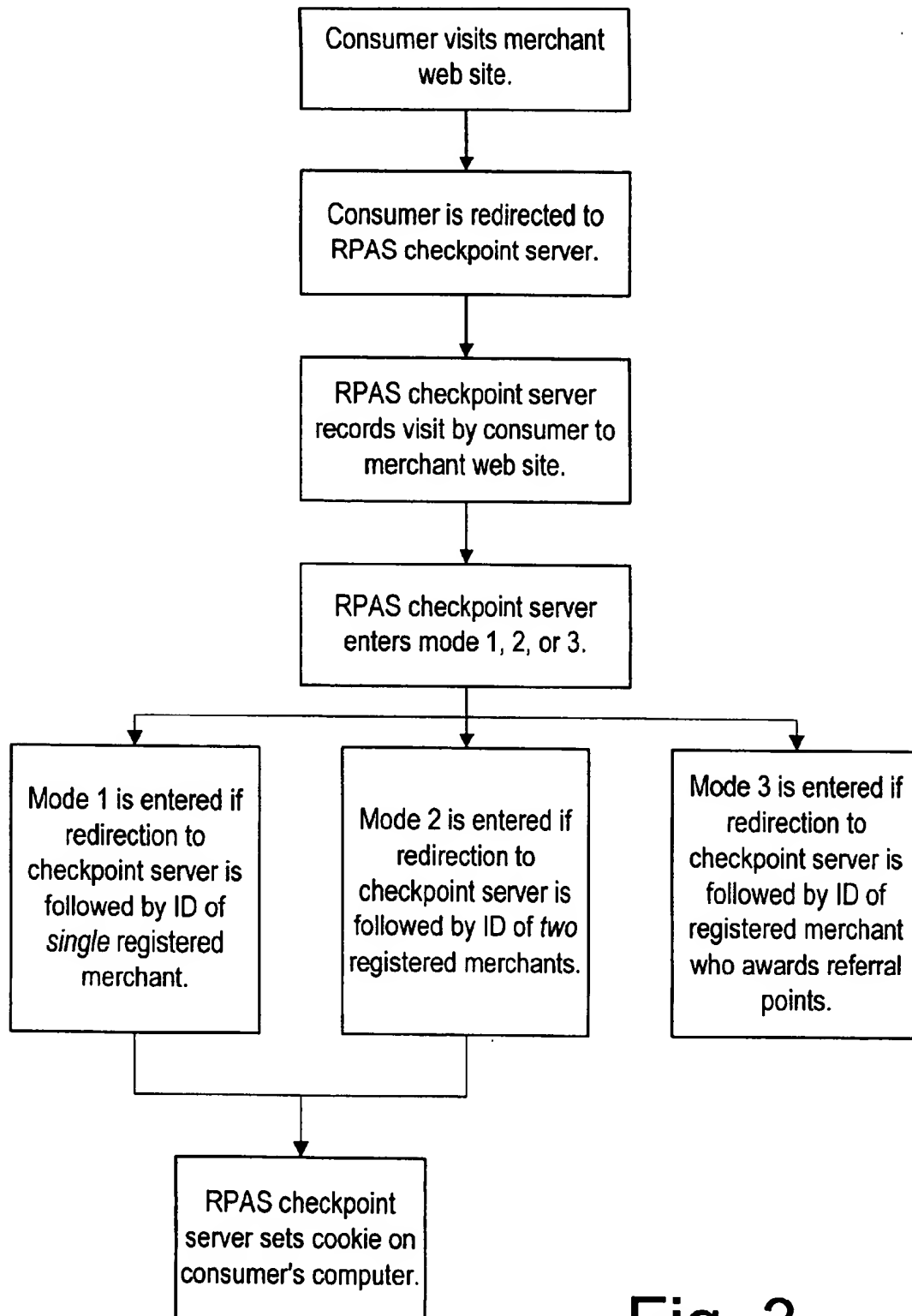
"Internet Micro-payment Protocols," by Chris A. Owen, date unknown (but prior to Jun. 9, 1977).
Downloaded information from "Cookie Central" website on the Internet, downloaded May 30, 1997.

"Micropayment Schemes Promise to Make the Web Profitable—One Penny at a Time," by Eric Brown, NewMedia, Jun. 23, 1997, pp. 1-7.

* cited by examiner

Fig. 1

Fig. 2Fig. 4

**Fig. 3**

METHOD AND ARCHITECTURE FOR MULTI-LEVEL COMMISSIONED ADVERTISING ON A COMPUTER NETWORK

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims priority from Provisional Application No. 60/079,223, filed Mar. 24, 1998.

FIELD OF THE INVENTION

The present invention pertains to the field of advertising on a computer network. More particularly, the present invention concerns how to reimburse a merchant operating an Internet server when a consumer has accessed the Internet server and then later accesses another Internet server operated by another merchant who has agreed to pay a referral fee.

BACKGROUND OF THE INVENTION

There are currently a number of advertising services in use on the Internet today. These advertising services facilitate buying and selling advertising space on merchant web sites. If a merchant wishes to buy advertising space (i.e. wishes to pay to have advertisements displayed on other web sites), the merchant contracts such an advertising service, negotiates a contract, and pays according to terms of the contract. If a merchant wishes to sell advertising space (i.e. wishes to get something of value in exchange for displaying advertisements for other merchants), the merchant registers with such an advertising service, then places special advertisement hyperlinks on the merchant's web site.

The term merchant is used here to indicate the owner or operator of a (computer) server linked to a network, such as the Internet, and able to publish information on the network. The information published by a first merchant could be pay-per-view information or an advertisement of goods and services offered by a first merchant, or the information could be an advertisement of goods and services offered by a second merchant, i.e. a referral to the second merchant. Various advertising systems have been developed to compensate a merchant for providing a referral to another merchant.

In many advertising systems, compensation to merchants who sell advertising space (i.e. who advertise for other merchants) is computed in one of three ways: per impression, per visitor, or per sale. Often an advertising service computes and distributes compensation. In the per impression way of computing compensation, such an advertising service counts the number of unique consumers who view the advertisement, and the merchant receives a fixed fee for each. Advertising services that use this method are currently located at the following web sites: <http://www.doubleclick.com>; <http://www.hyperbanner.com>; <http://www.linkexchange.com>; and <http://www.smartclicks.com>.

In the per visitor (consumer) way of computing compensation, an advertising service counts the number of unique consumers who click on the advertisement, and the merchant receives a fixed fee for each. Advertising services that use this method include: <http://www.aaddzz.com>; <http://www.bannerbrokers.com>; <http://www.clicktrade.com>; and <http://www.eads.com>.

In the per sale way of computing compensation, a merchant receives a commission when a consumer clicks on an advertising linking the consumer to the server of a merchant

and the consumer subsequently purchases goods or services from the merchant through the linked access.

On the Internet, computers access each other through the World Wide Web, a kind of network operating system. In this system, servers and consumer computers are said to reside at web sites. In the prior art of Internet advertising methods, it is common to use some standard procedure for identifying a consumer, or a consumer's computer, so as to track when the consumer accesses a merchant's web site, or when the consumer moves from one web page of a merchant (a quantity of intermission at a web site) to another (at possibly another web site). The tracking is performed by software put in place by the advertising service.

An advertising service may host, on a server operated by the advertising service, an actual advertisement for a merchant, as opposed to a link to an advertisement for the merchant. Then when a consumer selects to view, from a server operated by the merchant, a web page including an advertisement, the advertisement (i.e. the code for constructing its image for display as part of the web page) is actually pulled from the server of the advertising service by means of a link to the advertisement (in the code on the server, operated by the merchant, for constructing the web page). Thus, in an arrangement like this, the advertising service can record access by a consumer to an advertisement.

Alternatively, an advertising service may set up, on a first server operated by the advertising service itself, an advertisement for a merchant's web page stored on a server operated by the merchant, but which includes a link to a second server operated by the advertising service. Then a consumer who accesses the first server and selects to view the web page is directed to the second server operated by the advertising service, which then directs the consumer to the server operated by the merchant where the advertised web page is located. In this arrangement, the second server of the advertising service records access by the consumer of the advertised web page of the merchant.

Recording an access of an Internet server or of a web page on an Internet server is a feature of many commercial web servers. In providing this recording, such a web server may set, on consumer's computer, a so-called cookie (i.e. a persistent state data object, as described e.g. in U.S. Pat. No. 5,774,670) that distinguishes the consumer from other consumers, at least for subsequent accesses to a server in the same second-level Internet domain as the cookie-issuing web server. In the context of the present invention, a cookie is a data object that resides on a consumer's computer and can be updated by the web server that set the cookie on the consumer's computer. Such updating is performed to record, for example, a total number of visits, each visit by the consumer to the cookie-issuing web server. Whether or not a cookie is used in tracking a consumer, a web server may append, for later inspection, information about the consumer's computer (such as its network address) to a local log file (in memory or on storage media). Such consumer tracking is widely used, and is regarded as a valuable source of marketing information.

Thus, the consumer activity on the web leading up to viewing a merchant's web page does not flow according to any one particular structure at the code level; there are many ways a consumer might arrive at a web page, depending on what mechanisms the merchant and advertising service chose to use. In addition, there are many tracks through the web a consumer might take in ending up at a particular web site having a web page the consumer wants to view. A consumer might arrive at a web site by first looking up

3

information in a directory service or search engine. Or a consumer might arrive at a web site by following a helpful sequence of hyperlinks, possibly pointing to several other merchant web sites in the process.

"Because of this diversity of activity leading to a consumer viewing a particular web page, there is currently no robust mechanism to determine how the owner of the particular web page might compensate or credit merchants whose web sites were possibly instrumental in the consumer ultimately viewing the particular web page. What is needed is a way to determine what server-operating merchants to compensate, if any, for a consumer viewing a web page of another merchant who is willing to reward for potential referrals to the web page.

SUMMARY OF THE INVENTION

Accordingly, it is an object of the present invention to determine which server-operating merchants to reward in the event of a consumer accessing a web page of a merchant who desires to make compensation for referrals to the web page. It is a further object of the present invention to determine how much to reward such server-operating merchants.

The present invention achieves this object by a method, for use on a computer network, for distributing a reward from a paying merchant to participating merchants, the paying merchant and participating merchants all operating servers connected to the computer network, the reward to be distributed after a consumer visits a web site of the paying merchant, the method comprising the steps of: recording each access by the consumer of a participating merchant web site, including access by the consumer of the paying merchant web site; accepting referral points issued by a paying merchant when a consumer accesses a pre-determined web site of the paying merchant; and distributing to participating merchants the referral points according to criteria that limit the number of participating merchants, the criteria including a requirement that the consumer have visited a web site of a participating merchant before visiting the pre-determined web site of the paying merchant; wherein the distributing to participating merchants is calculated based on a pre-agreed pass-on percentage for each participating merchant, the pass-on percentage indicating what percentage of any referral points the participating merchant agrees to pass on to other participating merchants who satisfy the criteria for receiving a portion of the referral points.

In a particular embodiment of the present invention, the criteria include a requirement that the consumer visit a participating merchant within a pre-determined time before the consumer visits the pre-determined web site of the paying merchant in order for the participating merchant to be awarded a portion of the referral points.

In another embodiment of the present invention, the criteria include a requirement that after last visiting a participating merchant before the consumer visits the pre-determined web site of the paying merchant, the consumer not visit more than a pre-determined number of other participating merchants in order for the participating merchant to be awarded a portion of the referral points.

In another aspect of the present invention, the above object is achieved by an architecture, for use on a computer network, for distributing a reward from a paying merchant to participating merchants, the paying merchant and participating merchants all operating servers connected to the computer network, the reward to be distributed after a

4

consumer visits a web site of the paying merchant, the architecture comprising: means for recording each access by the consumer of a participating merchant web site, including access by the consumer of the paying merchant web site; means for accepting referral points issued by a paying merchant when a consumer accesses a pre-determined web site of the paying merchant; means for distributing to participating merchants the referral points according to criteria that limits the number of participating merchants, the criteria including a requirement that the consumer have visited a web site of a participating merchant before visiting the pre-determined web site of the paying merchant; wherein the means for distributing to participating merchants uses a pre-agreed pass-on percentage for each participating merchant, the pass-on percentage indicating what percentage of any referral points the participating merchant agrees to pass on to other participating merchants who satisfy the criteria for receiving a portion of the referral points.

In still another aspect of the present invention, the above object is achieved by an architecture, for use on a computer network, for executing a service of distributing a reward from a paying merchant to participating merchants, the paying merchant and participating merchants all operating servers connected to the computer network, the reward to be distributed after a consumer visits a web site of the paying merchant, the architecture comprising: a checkpoint server, for recording each access by the consumer of a participating merchant web site, including access by the consumer of the paying merchant web site; an accounting server, for accepting referral points issued by a paying merchant when a consumer accesses a pre-determined web site of the paying merchant, and for distributing to participating merchant the referral points according to criteria that limit the number of participating merchants, the criteria including a requirement that the consumer have visited a web site of a participating merchant before visiting the pre-determined web site of the paying merchant; and a merchant database server, for hosting a database of information about each participating merchant needed in performing the service, the information including a pass-on percentage, and for paying merchant also a number of referral points the paying merchant agrees to issue for distribution to participating merchants whenever a consumer visits an indicated web site of the paying merchant.

The present invention greatly extends the prior art notion of advertising on the Internet. The present invention is not intended to reward all merchants visited by a consumer on the way to a paying merchant, or even only those merchant actually instrumental in the consumer's visiting a web site of a paying merchant; it distributes rewards only approximately, making a tradeoff of accuracy for a lower burden of computation. The result is a means of compensating some merchants in a sequence of merchants who (only) potentially referred a consumer to a paying merchant, with little burden on system performance. Because the result provides compensation to more than the merchant operating the web site a consumer visits just before visiting the web site of a paying merchant, the present invention is said to provide multi-level commissioned advertising.

BRIEF DESCRIPTION OF THE DRAWINGS

The above and other features and advantages of the invention will become apparent from a consideration of the subsequent detailed description presented in connection with the accompanying drawings, in which:

FIG. 1 is a block diagram showing elements of an architecture used in compensating for referrals to a web page, according to the present invention;

5

FIG. 2 is a flow chart indicating how, according to the present invention, a merchant prepares to participate in a program providing referral fees;

FIG. 3 is a flow chart indicating how, according to the present invention, a merchant prepares to participate in a program providing referral fees; and

FIG. 4 is a flow chart showing one way according to the present invention to compensate merchants for referring a consumer to a web page of another merchant.

DESCRIPTION OF THE INVENTION INCLUDING BEST MODE

Referring now to FIG. 1, an architecture 13 for a referral reward program according to the present invention is shown. The program is operated by a referral point awarding service (RPAS). Merchants operating web sites on the Internet 15 register with the RPAS to become registered merchants. The referral award program rewards registered merchants who have potentially referred consumers to the web site of a registered merchant who has agreed to reward referral points through RPAS either when a consumer visits the web site of the paying merchant, or when a consumer has not only visited the web site, but actually purchased goods or services using the web site. Such a registered merchant is called here a paying merchant. The registered merchants who are eligible to receive a portion of the referral points are called here participating merchants. In the best mode, a registered merchant may be a participating merchant in one scenario (when a consumer accesses a server or visits a web site or accesses a particular web page of the registered merchant and eventually visits the web site of a paying merchant), and a paying merchant in another scenario (when a consumer accesses a server or visits a web site or accesses a particular web page of the registered merchant for which the registered merchant has agreed to award referral points). Each referral point represents something of value, such as frequent flyer miles or even money.

For the description provided here, a registered merchant will be either a participating merchant or a paying merchant (but not sometimes one and sometimes the other). But it is to be understood that, in the best mode, a registered merchant who has agreed to award referral points when a consumer ends up accessing material from a server of the registered merchant, can be a participating merchant in case of a consumer visiting some other paying merchant.

The architecture 13 includes various RPAS servers 10-12, connected to the Internet 15, including an RPAS accounting server 10 for awarding referral points when a suitable referral event occurs, an RPAS merchant database server 11 for hosting a database of participating merchants including information about the merchants relevant to the referral reward program, and an RPAS checkpoint server 12 for monitoring visits by consumers to web sites of the registered merchants. In the preferred embodiment, there are several checkpoint servers, each serving different merchants.

Connected to the architecture 13 through the Internet 15 are a consumer computer 14, and merchant web sites 1-k of registered merchants, the web sites indicated as merchant #1 web site 16, merchant #2 web site 17, merchant #3 web site 18, . . . , and merchant #k web site 19. Although other merchants (not shown) might also be connected to the Internet, it is assumed here that the merchants shown are all registered with the RPAS, as described below, and that at least one of these registered merchants is a paying merchant, i.e. one who has agreed to award referral points if a consumer accesses a server of the merchant or visits a particular web site of the merchant.

6

As a specific example of the present invention in the best mode, which will be described more specifically below, suppose that merchants m_1, m_2, m_3, and m_4 are the only merchants registered with RPAS, and suppose merchant m_4 agrees to award z=10 referral points when a consumer visits a web site of m_4, and that m_1, m_2 and m_3 are participating merchants in the scenario of this example. The referral points are to be distributed by RPAS among participating merchants, according to whether each of the other participating merchants is identified as meeting the criteria used in the present invention to award referral points.

As will be described below, each participating merchant has already agreed with RPAS to pass on some percentage of whatever referral points it is awarded. Suppose that the merchants m_1, m_2 and m_3 have agreed to pass on 30%, 25% and 40%, respectively, of whatever referral points are awarded to them.

Now suppose that a consumer visits the web sites of participating merchants m_1, m_2, m_3 and m_4 in that order, although not necessarily consecutively (i.e. the consumer might have also visited other web sites in touring these four web sites). As the consumer visits each of these web sites in turn, a checkpoint server 12 records the visit by entering either mode 1, mode 2, or mode 3, as will be described below. In this scenario, assume that the consumer does not click on an advertisement redirecting the consumer to m_4, but instead simply visits m_1, m_2, m_3 and m_4 in turn.

When the consumer computer 14 interfaces with the web site of m_4, the visit prompts m_4's server to send a request to the checkpoint server 12 to issue z=10 referral points. The checkpoint server 12 (operating in mode 3 as described below) then makes available to the accounting server 10 the recorded access information (i.e. that the consumer visited first m_1, then m_2, and so on) as well as the quantity of referral points paid by m_4. Finally, the accounting server 10 computes how to distribute the referral points. Based on the percentages of referral points m_1, . . . , m_4 have each agreed to pass on, the accounting server 10, tracing the path of the consumer backwards from m_4, passes on 40% of 10 points (=4 points) from m_3 (leaving m_3 with 6 points), passes on 25% of 4 points (=1 point) from m_2 (leaving m_2 with 3 points), and there being no more participating merchants to reward, leaves the remaining 1 point with m_1.

It is important to note that nowhere in the example was there a requirement that to earn a reward a merchant must have actually influenced the consumer to visit, sooner or later, the web site of m_4. In fact, the compensation would have been the same even if the consumer has ended up at m_4's web site purely by chance, i.e. without any suggestion, direct or indirect, by any of the "referring merchants" m_1, . . . , m_3. Thus, the method of the present invention for rewarding a participating merchant is based on the assumption that if a consumer visited the web site of a participating merchant and then after not having visited too many other web sites, ended up visiting a web site of a paying merchant, the participating merchant was part of the stream of influence that swept the consumer onto the web site of the paying merchant, and should therefore be awarded. In the best mode, a participating merchant would not receive a distribution of the referral points unless the consumer first visits a web site of the participating merchant, and then visits less than a certain pre-determined number of web sites of participating merchants, not necessarily different web sites, before visiting the web site of the paying merchant.

In another embodiment of the present invention, in order to foreclose as a possibility that a participating merchant would receive all of a distribution of referral points because a consumer repeatedly visits a web site of the participating merchant and then finally visits the web site of the paying merchant, the referral points are distributed to a predetermined number of different participating merchants. In this embodiment, for purposes of determining whether a particular participating merchant should receive a distribution of the referral points, only the last visit by a consumer to a web site of the participating merchant is taken into account.

In another embodiment, as an alternative to setting a cap on the number of last-visited participating merchants to which referral points are distributed, the present invention also comprehends setting a time limit on when a consumer can have visited a participated merchant and then have visited a paying merchant, to determine whether to award any referral points to the participating merchant. In yet another embodiment, there is both a time limit and a cap on the number of participating merchants that will receive a distribution of any referral points. In this, it is possible that a single participating merchant would receive all of a particular issue of referral points (if a consumer visits only the single participating merchant in the pre-determined time before visiting the paying merchant), and it is also possible that sometimes no referral points are awarded because no participating merchants satisfy the criteria for receiving a portion of an issue of the referral points.

In the best mode, with each participating merchant in the merchant database (maintained by the merchant database server 11) there are associated various items of information, including:

- a) a pass-on percentage, indicating, in a distribution of referral points, the percentage of the referral points received by the merchant that the merchant will pass on to other participating merchants;
- b) a checkpoint universal resource locator (url), i.e. a network address of the checkpoint server to be used by the merchant (not needed if all merchants use the same checkpoint server); alternatively, instead of a checkpoint url, a checkpoint server domain name (i.e. an alias for a url);
- c) at least one gateway url, i.e. a network address specified by the merchant to be the url of a web site of the merchant (the database accommodates a merchant having multiple web sites by using a relational database structure);
- d) an account balance, indicating the current total number of referral points earned by the merchant (and not yet redeemed); and
- e) a merchant identification, as a string of characters unique to the merchant, used for identifying the account holding the referral points for the merchant.

In the preferred embodiment, a merchant registers with RPAS (e.g. via phone, fax, email, or web) and selects a pass-on percentage. Each participating merchant then designs its web sites to trigger access by a consumer to the merchant's checkpoint server, using known methods of redirection in which a consumer is caused to access a merchant's checkpoint server by providing the consumer's computer with the checkpoint url, along with appended information.

In the preferred embodiment, a checkpoint server can operate in any of three modes whenever a consumer visits a participating or paying merchant. The particular mode used

by the checkpoint server depends on what merchants the consumer visits. In the preferred embodiment described here, the consumer visits web sites on the Internet and accesses web pages of servers operated by participating and paying merchants. The different modes will be here described in the preferred embodiment.

Mode 1 is entered by an RPAS checkpoint server when a consumer accesses a specially programmed web page of a participating merchant. The participating merchant will have embedded in the web page a data object that must be retrieved from a server operated by the RPAS in order for a browser, operated by the consumer on the consumer's computer, to build up the web page on the consumer's computer. The retrieval of such a data object from an RPAS server provides RPAS with the information it needs to track the consumer, i.e. to note that the consumer visited the particular participating merchant at a particular time. Mode 3 is entered in circumstances identical to those of mode 1, except that in mode 3 the consumer has visited a paying merchant, instead of a web page of merely a participating merchant. (Remember, both participating and paying merchants are "registered" with RPAS, and a registered merchant can be either a paying merchant or a participating merchant, depending on whether a consumer accesses a web page for which the registered merchant has agreed to award referral points.)

Mode 2 is entered by an RPAS checkpoint server when a consumer visits a web page of a participating merchant who embeds in the web page a data object that directs the consumer to another participating merchant, in what amounts to a true referral, but that first directs the consumer to an RPAS checkpoint server so that RPAS can note that the consumer first visited to the referring participating merchant, and then visited the referred to participating merchant.

In mode 1, the url of the checkpoint server provided to the consumer computer is followed by appended information that includes the identification of a single registered merchant, and the checkpoint server records that the consumer visited the identified merchant. Additionally, the checkpoint server sets a cookie (the persistent data object described above) on the consumer computer; the cookie has a timestamp and has the merchant identification appended to it. In applications where security is an important enough issue, the cookie is either encrypted or followed by an authentication string. After setting the cookie, the checkpoint server returns to the consumer computer a data object (essentially a web page and any associated information and scripts).

In mode 2, the checkpoint server address is followed by the identification of two registered merchants. The checkpoint server records that the consumer visited the first merchant, and then proceeded to the second merchant. Additionally the checkpoint server sets a cookie, with a timestamp and the two merchant identifications appended, on the consumer computer. The checkpoint server returns to the consumer computer data including a redirection causing the consumer computer to access the gateway url of the second merchant.

In mode 3, the checkpoint server address is followed by the identification of a single participating merchant and a number of referral points. The address also includes, in the best mode, a maximum number of participating merchants whom the paying merchant will compensate counting back from the participating merchant most recently visited by the consumer before visiting the paying merchant, and counting each participating merchant only once. Alternatively, the

address may instead include the value of a length of time, understood to be measured backward in time starting from when the consumer visits the web site of a paying merchant, beyond which a visit to a participating merchant by a consumer who later visits the paying merchant will not entitle the participating merchant to a share of any referral points made available by the paying merchant. (Here, a visit by a consumer to a merchant is intended to be understood to mean access by a consumer computer to a merchant web site.) The checkpoint server then proceeds as in mode 1, and also records a payment record ($z, m, c, t, \{n \text{ or } s\}$) indicating that z points have been provided to merchant m by virtue of consumer c accessing the paying merchant's server at time t , and should be distributed among the most recent n participating merchants visited by the consumer, or among all participating merchants visited by the consumer within the s seconds previous to the consumer visiting the paying merchant.

One skilled in the art can understand how to use the access records created by the checkpoint servers to construct a database of consumer movements. Specifically, for each consumer who has triggered an access to a checkpoint server, one can list the participating merchants the consumer has visited, in chronological order.

For each payment record ($z, m, c, t, \{s \text{ or } n\}$), using information obtained from the one or more checkpoint servers 12, the accounting server 10 considers the (possibly and acceptably incomplete) sequence of participating merchants accessed by consumer c . To eliminate anomalous behavior, in the preferred embodiment the accounting server may first filter through the sequence of participating merchants to remove those the consumer visited more than s second earlier than time t (when the consumer visited the paying merchant), and then removing all but one occurrence, such as the earliest occurrence, of each remaining participating merchant. In the case of using a maximum number n of to-be-compensated merchants, the RPAS accounting server filters out merchants visited by the consumer c earlier than the last n different participating merchants. Either way, the result of the filtering is a usually shortened list of merchants: m_1, m_2, \dots, m_k , where m_1 is the paying merchant, and m_k is the first participating merchant the consumer visits after time $t-s$, or no more than the n^{th} different participating merchant the consumer visits before visiting the paying merchant m_1 . (So the path of the consumer backward in time, is: m_1 (the paying merchant), then m_2 , and so on back to m_k .)

The accounting server 10 next redistributes the z referral points to the merchants in the filtered list according to one or another algorithm. In the best mode, the accounting server distributes the referral points among the participating merchants earning referral points based on the pass-on percentage of each such merchant, as in the example discussed above (involving m_1, \dots, m_4 , where m_1 is the paying merchant, and m_2 is the participating merchant the consumer visited just before visiting the paying merchant m_4 , and so on). Such a distribution is expressed algorithmically in FIG. 4. In addition to the procedural steps shown in FIG. 4, the accounting server may perform rounding up or down of referral points to be awarded, or may deduct service charges.

Note that the accounting server 10 has all the information needed to prepare a pass-on list, i.e. a list providing referral points passed on to others by each participating merchant during a predetermined time interval. Thus, the RPAS can prepare such a list for use by the registered merchants to help them determine how to optimize the value of the referrals they make.

It is to be understood that the above described arrangements are only illustrative of the application of the principles of the present invention. In particular, the present invention is intended to comprehend criteria for determining which participating merchants should receive at least some of an issue of referral points can be fashioned where the criteria include the possibility that even if only a single participating merchant is eligible, only a fraction of the issued referral points are distributed. Numerous other modifications and alternative arrangements may be devised by those skilled in the art without departing from the spirit and scope of the present invention, and the appended claims are intended to cover such modifications and arrangements.

What is claimed is:

1. A method, for use on a computer network, for distributing a reward from a paying merchant to participating merchants, the paying merchant and participating merchants all operating servers connected to the computer network, the reward to be distributed after a consumer visits a web site of the paying merchant, the method comprising the steps of:

- a) recording each access by the consumer of a participating merchant web site, including access by the consumer of the paying merchant web site;
- b) accepting referral points issued by the paying merchant when a consumer accesses a pre-determined web site of the paying merchant; and
- c) distributing to participating merchants the referral points according to criteria that limit the number of participating merchants, the criteria including a requirement that the consumer have visited a web site of a participating merchant before visiting the pre-determined web site of the paying merchant; and

wherein the distributing to participating merchants is calculated based on a pre-agreed pass-on percentage for each participating merchant, the pass-on percentage indicating what percentage of any referral points the participating merchant agrees to pass on to other participating merchants who satisfy the criteria for receiving a portion of the referral points.

2. The method claimed in claim 1, wherein the criteria include a requirement that the consumer visit a participating merchant within a pre-determined time before the consumer visits the pre-determined web site of the paying merchant in order for the participating merchant to be awarded a portion of the referral points.

3. The method claimed in claim 1, wherein the criteria include a requirement that after last visiting a participating merchant before the consumer visits the pre-determined web site of the paying merchant, the consumer not visit more than a pre-determined number of other participating merchants in order for the participating merchant to be awarded a portion of the referral points.

4. An architecture, for use on a computer network, for distributing a reward from a paying merchant to participating merchants, the paying merchant and participating merchants all operating servers connected to the computer network, the reward to be distributed after a consumer visits a web site of the paying merchant, the architecture comprising:

- a) means for recording each access by the consumer of a participating merchant web site, including access by the consumer of the paying merchant web site;
- b) means for accepting referral points issued by the paying merchant when a consumer access a pre-determined web site of the paying merchant;
- c) means for distributing to participating merchants the referral points according to criteria that limits the

11

number of participating merchants, the criteria including a requirement that the consumer have visited a web site of a participating merchant before visiting the pre-determined web site of the paying merchant; wherein the means for distributing to participating merchants uses a pre-agreed pass-on percentage for each participating merchant, the pass-on percentage indicating what percentage of any referral points the participating merchant agrees to pass on to other participating merchants who satisfy the criteria for receiving a portion of the referral points.

5. The architecture of claim 4, wherein the criteria includes a requirement that the consumer visit a participating merchant within a pre-determined time before the consumer visits the pre-determined web site of the paying merchant in order for the participating merchant to be awarded a portion of the referral points.

6. The architecture of claim 4, wherein the criteria includes a requirement that after last visiting a participating merchant before the consumer visits the pre-determined web site of the paying merchant, the consumer not visit more than a pre-determined number of other participating merchants in order for the participating merchant to be awarded a portion of the referral points.

7. An architecture, for use on a computer network, for executing a service of distributing a reward from a paying merchant to participating merchants, the paying merchant and participating merchants all operating servers connected to the computer network, the reward to be distributed after a consumer visits a web site of the paying merchant, the architecture comprising:

- a) a checkpoint server, for recording each access by the consumer of a participating merchant web site, including access by the consumer of the paying merchant web site;

12

- b) an accounting server, for accepting referral points issued by the paying merchant when a consumer accesses a pre-determined web site of the paying merchant, and for distributing to participating merchants the referral points according to criteria that limit the number of participating merchants, the criteria including a requirement that the consumer have visited a web site of a participating merchant before visiting the pre-determined web site of the paying merchant; and

- c) a merchant database server, for hosting a database of information about each participating merchant needed in performing the service, the information including a pass-on percentage, and for a paying merchant also a number of referral points the paying merchant agrees to issue for distribution to participating merchants whenever a consumer visits an indicated web site of the paying merchant.

8. The architecture of claim 7, wherein the criteria include a requirement that the consumer visit a participating merchant within a pre-determined time before the consumer visits the pre-determined web site of the paying merchant in order for the participating merchant to be awarded a portion of the referral points.

9. The architecture of claim 7, wherein the criteria include a requirement that after last visiting a participating merchant before the consumer visits the pre-determined web site of the paying merchant, the consumer not visit more than a pre-determined number of other participating merchants in order for the participating merchant to be awarded a portion of the referral points.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 6,289,318 B1
DATED : September 11, 2001
INVENTOR(S) : Timothy P. Barber

Page 1 of 1

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 1,

Line 27, "contracts" should be -- contacts --

Line 67, "advertising" should be -- advertisement --

Column 4,

Line 30, "sire" should be -- site --

Line 31, second occurrence of "merchant" should be -- merchants --

Line 39, before "paying" -- a -- should be inserted

Line 47, second occurrence of "merchant" should be -- merchants --

Column 6,

Line 43, after "and" -- , -- should be inserted

Column 9,

Line 31, "second" should be -- seconds --

Column 10, claim 1,

Line 32, "and" should be deleted

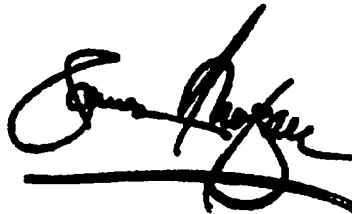
Column 10, claim 4,

Line 64, "access" should be -- accesses --

Signed and Sealed this

Twelfth Day of March, 2002

Attest:



Attesting Officer

JAMES E. ROGAN
Director of the United States Patent and Trademark Office